Journal of Air Transport Management 35 (2014) 19–28

Contents lists available at ScienceDirect

Journal of Air Transport Management

journal homepage: www.elsevier.com/locate/jairtraman

Cost-benefit analysis of airport security: Are airports too safe?

Mark G. Stewart [a,*], John Mueller [b,c,1]

[a] Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales 2308, Australia
[b] Mershon Center for International Security Studies, Ohio State University, USA
[c] Cato Institute, Washington, D.C., USA

Keywords:
Risk
Cost-benefit analysis
Airports
Security
Terrorism

A B S T R A C T

This paper assesses the risks and cost-effectiveness of measures designed to further protect airport terminals and associated facilities such as car parks from terrorist attack in the U.S., Europe, and the Asia-Pacific area. The analysis considers threat likelihood, the cost of security measures, hazard likelihood, risk reduction and expected losses to compare the costs and benefits of security measures to decide the optimal security measures to airports. Monte-Carlo simulation methods were used to propagate hazard likelihood, risk reduction and loss uncertainties in the calculation of net benefits that also allows probability of cost-effectiveness to be calculated. It is found that attack probabilities had to be much higher than currently observed to justify additional protective measures. Overall, then, it is questionable whether special efforts to further protect airports are sensible expenditures. Indeed, some relaxation of the measures already in place may well be justified.

1. Introduction

Much research on aviation security focuses on airplanes due no doubt to the events of September 11 2001 and to the more recent attempts to bomb U.S. bound flights in 2001, 2006 and 2009. Although there may be special reasons to protect airplanes, however, it is not at all clear that there are any special reasons to protect airports. Elias (2010) states that these areas have 'unique vulnerabilities because it is unsecured'. However, compared with many other places of congregation, people are more dispersed in airports, and therefore a terrorist attack is likely to kill far fewer than if, for example, a crowded stadium is targeted. The 2011 suicide bombing in the baggage claim area of Moscow's Domodedovo airport did kill 37 and injure many others, and this shows that airports are not unattractive targets. However, in the previous year suicide bombers targeted the Moscow metro killing 25, and the year before that, derailed the Moscow to St. Petersburg high-speed train killing 27.

In the fourteen year period 1998–2011, the Global Terrorism Database recorded 20 attacks on airports in the U.S. and Europe, killing 64 people. Notable among these are the attempted bombing of the Glasgow international airport in 2007 and the shooting of two people at the El Al ticket counter at Los Angeles International Airport (LAX) in 2002. Over the same period there were 31 attacks on aircraft. In total, attacks on aviation accounts for only 0.5% of all terrorist attacks, and attacks on airports comprise less than half of these. This experience has led the 2007 U.S. National Strategy for Aviation Security to conclude that 'reported threats to aviation infrastructure, including airports and air navigation facilities are relatively few.' A study of 53 cases that have come to light since 9/11 in which Muslim terrorists planned, or in many cases vaguely imagined, doing damage in the United States finds only two in which an airport facility was on the target list (Mueller, 2013).

A risk and cost-benefit assessment quantifies risk reduction of security measures, losses from a successful attack, threat likelihood, probability that attack is successful, and cost of security measures. This allows costs and benefits of security measures to be compared and optimal security measures to be selected. In earlier work evaluating in-flight airline security measures we have considered cost per life saved as the sole decision-support criterion (Stewart and Mueller, 2008), and we later conducted a systems reliability analysis with a more detailed cost-benefit assessment that included other losses from a terrorist attack (Stewart and Mueller, 2013a,b; see also Jackson et al., 2012). These analyses considered single point estimates of risk reduction and losses. In this paper, we characterise probability of attack success, risk reduction, and losses as probabilistic variables allowing confidence intervals to be calculated (for preliminary efforts, see Stewart and Mueller, 2011). For a literature review of probabilistic terrorism risk assessment see Stewart and Mueller (2013a).

* Corresponding author. Tel.: +61 2 49216027.
E-mail addresses: mark.stewart@newcastle.edu.au (M.G. Stewart), bbbb@osu.edu (J. Mueller).
[1] Tel.: +1 614 2476007.

0969-6997/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jairtraman.2013.11.003

The U.S. Transportation Security Administration (TSA) has extensive security guidelines for airport planning, design and construction (TSA, 2011). However, there is little information about whether TSA guidelines satisfy a cost-benefit assessment. The U.S. Government Accountability Office and Congress have repeatedly urged the TSA to undertake risk and cost-benefit assessments of major programmes (GAO, 2011; Rogers, 2012). The TSA has used the Risk Management Analysis Tool (RMAT) to conduct risk assessments. However, a review by RAND (Morral et al., 2012) revealed a number of key deficiencies. Among them: 'RMAT does not attempt to describe the absolute risks to the system, rather just the relative risks, or changes in magnitude of risk', and thus RMAT can only 'partially meet' TSA needs. What is needed is a methodology that can assess absolute risk and risk reduction. A key component of assessing absolute risk is including the probability of an attack in the calculations, whereas a relative risk assessment is often conducted conditional on an attack occurring and then ranking risks based on the relative likelihood of threats.

This paper seeks to assess the absolute risks and cost-effectiveness of measures designed to protect airport terminals and associated facilities such as car parks from terrorist attack. These are areas where the general public has unrestricted access to before passengers undertake security screening and pass into secured (sterile) areas prior to aircraft boarding. We rely extensively on cost and risk reduction data for LAX compiled by RAND in 2004 (Stevens et al., 2004), which considered bombings or shooting attacks at the airport curbside or in other pre-screening areas of passenger terminal buildings. We evaluate security measures such as reducing congestion by additional check-in staff and TSA screening lines, making buildings blast-resistant, and screening of vehicles and luggage for IEDs (Improvised Explosive Devices). These range in cost from $2.5 to $60 million per airport per year. LAX is the sixth busiest airport in the world, and third busiest in the United States. Hence, LAX represents a typical large international airport in a class with London Heathrow, New York JFK, and Washington Dulles airports.

The paper first explains risk-based decision theory, and then describes the threats that airport terminal buildings are exposed to, enhanced security measures to deal with these threats, and their cost. The risk reduction for enhanced security measures, loss likelihood, and losses sustained in a successful attack are then inferred. Fatality risks, net present value and benefit-to-cost ratio are calculated for various attack probabilities. The probability of cost-effectiveness is also calculated. This allows the cost-effectiveness of security measures to be assessed and compared, and optimal security measures selected.

2. Risk-based decision theory

2.1. Definition of risk

A standard definition of risk or expected loss is:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequences} \tag{1}$$

This is consistent with the conceptual framework adopted by the TSA (NRC, 2010) and risk analyses for many applications (e.g., Kaplan and Garrick, 1981; Stewart and Melchers, 1997). This leads to a simplified formulation for risk:

$$E(L) = \sum \Pr(T)\Pr(L|T)L \tag{2}$$

where $\Pr(T)$ is the annual *threat* probability per target, $\Pr(L|T)$ is the conditional probability of loss (that the explosive will be successfully detonated or the gun will fire leading to damage and loss of life) given occurrence of the threat (*vulnerability*), and L is the loss or *consequence* (i.e., damage costs, number of people exposed to the hazard) if the attack is 100% successful. The summation sign in Eqn. (2) refers to the number of possible threats and losses.

Each threat has a certain relative likelihood $\Pr(T|\text{attack})$ such that $\Pr(T) = p_{\text{attack}} \times \Pr(T|\text{attack})$ where p_{attack} is the annual probability of attack absent of the security measure. Note that $\Pr(L|T)$ represents the likelihood that a terrorist will succeed in creating the desired hazard and loss. This will be influenced by task complexity (degree of difficulty in planning, acquiring materials, and carrying out an attack), competency of the individual, and security measures. If the attack is successful in achieving the desired effect and maximum losses then $\Pr(L|T) = 100\%$.

2.2. Cost-effectiveness of security measures

Three criteria may be used to compare the cost-effectiveness of adaptation strategies:

1. Net Present Value or NPV
2. Benefit-to-cost ratio or BCR
3. Break-even analysis that assesses how high the probability of an otherwise successful attack needs to be for a security measure to begin to be cost-effective or $\Pr(\text{BCR} > 1)$ or $\Pr(\text{NPV} > 0)$

The 'benefit' of a security measure is the losses averted due to the security measure, and the 'cost' is the cost of the security measure. The net present value NPV (or net benefit) is equal to benefit minus the cost. The decision problem is to maximise the net present value

$$\text{NPV} = \sum E(L)\Delta R + \Delta B - C_{\text{security}} \tag{3}$$

where ΔR is the reduction in risk caused by security measures, C_{security} is the cost of security measures including opportunity costs that reduces risk by ΔR, ΔB is the expected co-benefit from the security measure not directly related to mitigating vulnerability or hazard (such as reduction in crime, improved passenger experience, etc), and $E(L)$ is the 'business as usual' expected loss (risk) given by Eqn. (2). The risk reduction (ΔR) may arise from a combination of reduced likelihood of threat or hazard or loss, and can vary from 0% to 100%.

A complementary decision metric is the benefit-to-cost ratio

$$\text{BCR} = \frac{\sum E(L)\Delta R + \Delta B}{C_{\text{security}}} \tag{4}$$

Maximising NPV (but not BCR) will lead to optimal outcomes when prioritising the cost-effectiveness of various security measures (e.g., OMB, 1992). In terms of risk communication, the concept of a BCR has some appeal to policy makers. However, prioritising security measures based on maximising BCR may lead to sub-optimal outcomes as a high BCR can be achieved if the cost is small, but NPV may be lower than other security measures (OMB, 1992; OBPR, 2009). There are some advantages to BCR, as the Australian Government Office of Best Practice and Regulation explains "BCR is only preferred to NPV in situations where capital projects need to be funded from a limited pool of funds. In this case, it can be shown that allocating funds by way of the BCR criterion results in a higher net social benefit than by using NPV. However, regulatory CBA [cost benefit analysis] rarely deals with making capital investments from fixed funding pools." (OBPR, 2009). Either way, if a security measure has $\text{NPV} > 0$ then clearly $\text{BCR} > 1$.

We recognise that perceptions of risk and risk averseness are commonly cited as reasons to overinvest in homeland security